J.W. Price 949/261-8433
Yuichi Futa
S.N. 09/603,636

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

NAK1-BL53

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９９年 ７月１６日

出願番号
Application Number: 平成１１年特許願第２０３０５５号

出願人
Applicant (s): 松下電器産業株式会社

２０００年 ６月２９日

特許庁長官
Commissioner,
Patent Office 近藤隆彦

【書類名】　特許願
【整理番号】　2022510334
【提出日】　平成11年 7月16日
【あて先】　特許庁長官殿
【国際特許分類】　G09C　5/00
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　布田　裕一
【特許出願人】
　【識別番号】　000005821
　【氏名又は名称】　松下電器産業株式会社
【代理人】
　【識別番号】　100097445
　【弁理士】
　【氏名又は名称】　岩橋　文雄
【選任した代理人】
　【識別番号】　100103355
　【弁理士】
　【氏名又は名称】　坂口　智康
【選任した代理人】
　【識別番号】　100109667
　【弁理士】
　【氏名又は名称】　内藤　浩樹
【手数料の表示】
　【予納台帳番号】　011305
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9809938

【プルーフの要否】　不要

【書類名】　明細書

【発明の名称】　有限体上の演算装置、逆元演算装置および暗号システム

【特許請求の範囲】

【請求項１】　予め与えられた有限体GF(p)(p:素数)において、正の整数nと、GF(p)上のn元連立一次方程式のパラメータa↓(ij)(1≦i、j≦n)、b↓k(1≦k≦n)を入力とし、前記方程式の解を出力する有限体上の演算装置であって、

前記連立方程式を行列と第１のベクトルで表現し、前記行列と前記第１のベクトルを出力する第１方程式変換部と、

前記第１方程式変換部から出力される前記行列を三角化変換するために、前記行列と前記第１のベクトルを変換し、変換された三角行列と第２のベクトルを出力する第２方程式変換部と、

前記第２方程式変換部から出力される前記三角行列の対角成分のGF(p)上の逆元を出力する逆元演算部と、

前記第２方程式変換部から出力される三角行列と前記第２のベクトルと、前記逆元演算部から出力される逆元を用いて前記n元連立一次方程式の解を求める方程式求解部とを備え、

前記第２方程式変換部では、前記有限体の逆元演算を行わないことを特徴とする有限体上の演算装置。

【請求項２】　前記逆元演算部は、前記第２方程式変換部から出力される三角行列の対角成分をm↓1、m↓2、...、m↓nとし、出力するGF(p)上の逆元をI↓1、...、I↓nとするとき、

$$t\downarrow i=\prod\downarrow(k\neq i)\ m\downarrow k \bmod p \qquad (i=1、2、\ldots、n)$$

と

$$t=\prod\downarrow k\ m\downarrow k \bmod p$$

を計算する乗算手段と、

$$u=1/t \bmod p$$

を計算する第１逆元演算手段と、

$$I\downarrow i = u\times t\downarrow i \bmod p \qquad (i=1、2、\ldots、n)$$

を計算する第２逆元演算手段からなることを特徴とする請求項１記載の有限体上

の演算装置(ただし、x↓1はxの下付き添字が1であることを示す)。

【請求項３】　前記乗算手段は、前記t↓i(i=1、2、...、n)を

s↓1=m↓1×m↓2 mod p

s↓2=s↓1×m↓3 mod p

...

s↓(n-3)=s↓(n-4)×m↓(n-2) mod p

t↓n=s↓(n-3)×m↓(n-1) mod p

t↓(n-1)=s↓(n-3)×m↓n mod p

s↓n=m↓(n-1)×m↓n mod p

t↓(n-2)=s↓(n-4)×s↓n mod p

s↓(n-1)=m↓(n-2)×s↓n mod p

t↓(n-3)=s↓(n-5)×s↓(n-1) mod p

s↓(n-2)=m↓(n-3)×s↓(n-1) mod p

t↓(n-4)=s↓(n-6)×s↓(n-2) mod p

...

s↓5=m↓4×s↓6 mod p

t↓3=s↓1×s↓5 mod p

s↓4=m↓3×s↓5 mod p

t↓2=m↓1×s↓4 mod p

t↓1=m↓2×s↓4 mod p

により計算し、tを予め与えられたkを用いて、

t=t↓k×m↓k

により計算することを特徴とする請求項２記載の有限体上の演算装置。

【請求項４】　予め与えられた有限体GF(p)の拡大体GF(q)(q=p↑n)において、GF(q)の元xを入力とし、xのGF(q)上の逆元を出力する逆元演算装置であって、

前記元xを入力とし、前記元xの逆元を求めるための連立方程式を生成する方程式生成部と、

前記方程式生成部から出力される連立方程式の解を求める方程式計算部と、

前記方程式計算部の解をxの逆元に変換する逆元変換部とを備え、

前記方程式計算部は請求項１記載の有限体上の演算装置であることを特徴とする逆元演算装置(ただし、p↑nはpのn乗を示す)。

【請求項５】　予め与えられた有限体GF(p)の拡大体GF(q)(q=p↑n)において、GF(q)の元xを入力とし、xのGF(q)上の逆元を出力する逆元演算装置であって、

前記元xを入力とし、前記元xの逆元を求めるための連立方程式を生成する方程式生成部と、

前記方程式生成部から出力される連立方程式の解を求める方程式計算部と、

前記方程式計算部の解をxの逆元に変換する逆元変換部を備え、

前記方程式計算部は請求項２記載の有限体上の演算装置であることを特徴とする逆元演算装置。

【請求項６】　予め与えられた有限体GF(p)の拡大体GF(q)(q=p↑n)において、GF(q)の元xを入力とし、xのGF(q)上の逆元を出力する逆元演算装置であって、

前記元xを入力とし、前記元xの逆元を求めるための連立方程式を生成する方程式生成部と、

前記方程式生成部から出力される連立方程式の解を求める方程式計算部と、

前記方程式計算部の解をxの逆元に変換する逆元変換部とを備え、

前記方程式計算部は請求項３記載の有限体上の演算装置であることを特徴とする逆元演算装置。

【請求項７】　予め与えられた有限体GF(p)を利用する有限体利用暗号システムであって、

有限体上の暗号装置と、

正の整数nとGF(p)上のn元連立一次方程式のパラメータa↓(ij)(1≦i、j≦n)、b↓k(1≦k≦n)を入力とし、前記方程式の解を出力する連立方程式求解装置とを備え、

前記連立方程式求解装置は請求項１記載の有限体上の演算装置であることを特徴とする有限体利用暗号システム。

【請求項８】　予め与えられた有限体GF(p)を利用する有限体利用暗号システムであって、

有限体を上の暗号装置と、

正の整数nとGF(p)上のn元連立一次方程式のパラメータa↓(ij)(1≦i、j≦n)、b↓k(1≦k≦n)を入力とし、前記方程式の解を出力する連立方程式求解装置とを備え、

前記連立方程式求解装置は請求項２記載の有限体上の演算装置であることを特徴とする有限体利用暗号システム。

【請求項９】　予め与えられた有限体GF(p)を利用する有限体利用暗号システムであって、

有限体上の暗号装置と、

正の整数nとGF(p)上のn元連立一次方程式のパラメータa↓(ij)(1≦i、j≦n)、b↓k(1≦k≦n)を入力とし、前記方程式の解を出力する連立方程式求解装置とを備え、

前記連立方程式求解装置は請求項３記載の有限体上の演算装置であることを特徴とする有限体利用暗号システム。

【請求項１０】　予め与えられた有限体GF(p)の拡大体GF(q)(q=p↑n)を利用する拡大体利用暗号システムであって、

拡大体上の暗号装置と、

GF(q)の元xを入力とし、xのGF(q)上の逆元を出力する逆元演算装置とを備え、

前記逆元演算装置は請求項４記載の逆元演算装置であることを特徴とする拡大体利用暗号システム。

【請求項１１】　予め与えられた有限体GF(p)の拡大体GF(q)(q=p↑n)を利用する拡大体利用暗号システムであって、

拡大体上の暗号装置と、

GF(q)の元xを入力とし、xのGF(q)上の逆元を出力する逆元演算装置とを備え、

前記逆元演算装置は請求項５記載の逆元演算装置であることを特徴とする拡大体利用暗号システム。

【請求項１２】　予め与えられた有限体GF(p)の拡大体GF(q)(q=p↑n)を利用する拡大体利用暗号システムであって、

拡大体上の暗号装置と、

GF(q)の元xを入力とし、xのGF(q)上の逆元を出力する逆元演算装置とを備え、

前記逆元演算装置は請求項６記載の逆元演算装置であることを特徴とする拡大体利用暗号システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は情報セキュリテイ技術としての暗号技術及び、誤り訂正技術に関するものであり、特に、拡大体および連立方程式を用いて実現する暗号及びデジタル署名技術、誤り訂正技術に関するものである。

【０００２】

【従来の技術】

秘密通信方式とは、特定の通信相手以外に通信内容を漏らすことなく通信を行なう方式である。またデジタル署名方式とは、通信相手に通信内容の正当性を示したり、本人であることを証明する通信方式である。この署名方式には公開鍵暗号とよばれる暗号方式を用いる。公開鍵暗号は通信相手が多数の時、通信相手ごとに異なる暗号鍵を容易に管理するための方式であり、多数の通信相手と通信を行なうのに不可欠な基盤技術である。簡単に説明すると、これは暗号化鍵と復号化鍵が異なり、復号化鍵は秘密にするが、暗号化鍵を公開する方式である。この公開鍵暗号の安全性の根拠に用いられるものに離散対数問題がある。離散対数問題には代表的に、有限体上定義されるもの及び楕円曲線上定義されるものがある。これはNeal Koblitz,"A Course in Number theory and Cryptography",Springer-Verlag,1987に詳しく述べられている。楕円曲線上の離散対数問題を以下に述べる。

【０００３】

楕円曲線上の離散対数問題とは、

Eを有限体GF(q)(q=p↑n、p:素数)上定義された楕円曲線とし、Eの位数が大きな素数で割れる元Gをベースポイントとする(p↑nはpのn乗を示す)。このとき、Eの与えられた元Yに対して、

$$Y=x*G$$

となる整数xが存在するならばxを求めよ、という問題である(ここで、x＊GはGを

x回楕円曲線の加算を行うことを意味する)。ここで、GF(q)はGF(p)の拡大体である。拡大体については、岡本龍明、山本博資、"現代暗号"、シリーズ／情報科学の数学、産業図書、1997、26～28ページに詳しく述べられている。

【０００４】

(従来例１)

以下に上記楕円曲線上の離散対数問題を応用したエルガマル署名について、図６を用いて説明する。

【０００５】

この図は、上記エルガマル署名によるデジタル署名方式の手順を示すシーケンス図である。

【０００６】

ユーザA310、管理センタ320及びユーザB330は、ネットワークで接続されている。

【０００７】

pを素数、q=p↑n、有限体GF(q)上の楕円曲線をEとする。Eのベースポイントを Gとし、Gの位数をrとする。すなわち、rは、

r＊G=0

を満たす最小の正整数である。ただし、0は楕円曲線の群の加算における零元である。

【０００８】

(1)管理センタ320による公開鍵の生成

管理センタ320は、予め通知されているユーザA310の秘密鍵x↓Aを用いて、次の式より、ユーザA310の公開鍵を作成する(ステップS1～S2)。

【０００９】

Y↓A=x↓A＊G

その後、管理センタ320は、有限体GF(q)、楕円曲線E及びベースポイントGをシステムパラメータとして公開し、他のユーザB330にユーザA310の公開鍵Y↓Aを公開する(ステップS3～S4)。

【００１０】

(2)ユーザA310による署名生成

ユーザA310は、乱数kを生成する(ステップS5)。

【００１１】

次に、ユーザA310は、

$R\downarrow 1=(r\downarrow x,\ r\downarrow y)=k*G$

を計算し(ステップS6)、

$s\times k=m+r\downarrow x\times x\downarrow A \mod r$

から、sを計算する(ステップS7)。ここで、mは、ユーザA310がユーザB330へ送信するメッセージである。

【００１２】

さらに、ユーザA310は、得られた(R↓1、s)を署名としてメッセージmとともに、ユーザB330へ送信する(ステップS8)。

【００１３】

(3)ユーザB330による署名検証

ユーザB330は、

$s*R\downarrow 1=m*G+r\downarrow x*Y\downarrow A$

が成立するかどうか判定することにより、送信者であるユーザA310の身元を確認する(ステップS9)。これは、

$$s*R\downarrow 1=[((m+r\downarrow x\times x\downarrow A)/k)\times k]*G$$
$$=(m+r\downarrow x\times x\downarrow A)*G$$
$$=m*G+(r\downarrow x\times x\downarrow A)*G$$
$$=m*G+r\downarrow x*Y\downarrow A$$

となることから明らかである。

【００１４】

上記に示した楕円曲線上の離散対数問題を応用したエルガマル署名によるデジタル署名方式における公開鍵の生成、署名生成、署名検証のそれぞれにおいて、楕円曲線上の点の冪倍の演算が行われる。

【００１５】

楕円曲線の演算公式については、

Miyaji, Ono, and Cohen,

"Efficient elliptic curve exponentiation",

Advances in cryptology-proceedings of ICICS'97,

Lecture notes in computer science, 1997, Springer-verlag, 282-290.

に詳しく説明されている。

【００１６】

楕円曲線の方程式を

y↑2=x↑3+a×x+b

とする。任意の楕円曲線上の点Pの座標を(x↓1、y↓1)とする。この座標はアフィン座標と呼ばれ、楕円曲線の加算に有限体GF(q)の逆元演算の処理を含むことが知られている。上記の論文では、射影座標と呼ばれる座標に触れているが、これは、

(x↓1、y↓1)→ (x↓1、y↓1、1)

と2項組座標を3項組座標に対応づけるものである。逆に、

(X、Y、Z)→ (X/Z、Y/Z)

と対応する。3項組座標の場合、楕円曲線の加算に有限体GF(q)の逆元演算の処理を含まない。一般に有限体の逆元演算は、計算時間が大きいため、3項組座標をよく用いられる。

【００１７】

しかし、この座標もエルガマル署名に使用する場合は、ステップS6のようにアフィン座標に変換する必要がある。したがって、この場合も逆元演算が必要になる。

【００１８】

このため、逆元演算の処理時間を削減することは、楕円曲線暗号の高速化につながる。しかし、従来の逆元演算法は処理時間が長いという問題がある。

【００１９】

(従来例２)

以下で、従来の拡大体GF(q)(q=p↑n、p:素数)の逆元演算について図７を用いて説明する。ここで、簡単のため拡大体GF(q)の生成多項式をf(g)=g↑n-βとし

、生成多項式の根をαとする。入力となるGF(q)の元をx=x↓0+x↓1×α+...+x↓(n-1)×α↑(n-1)とする。

【００２０】

step1:方程式生成部401

xから以下のy↓i(0≦i≦n-1)に関する連立方程式を生成する。

【００２１】

x↓0×y↓0+β×x↓(n-1)×y↓1+β×x↓(n-2)×y↓2+...+β×x↓1×y↓(n-1)=1

x↓1×y↓0+x↓0×y↓1+β×x↓(n-1)×y↓2+...+β×x↓2×y↓(n-1)=0

x↓2×y↓0+x↓1×y↓1+x↓0×y↓2+...+β×x↓3×y↓(n-1)=0

...

x↓(n-1)×y↓0+x↓(n-2)×y↓1+x↓(n-3)×y↓2+...+x↓0×y↓(n-1)=0

step2:方程式計算部402

方程式生成部401で生成した方程式の解y↓k(0≦k≦n-1)を求める。

【００２２】

step3:逆元変換部403

方程式計算部402で求めた解y↓k(0≦k≦n-1)を逆元I=y↓0+y↓1×α+...+y↓(n-1)×α↑(n-1)に変換する。

【００２３】

上記のIとxについて、

x×I=1 mod f(g)

という関係式であるとき、

x×I=x↓0×(y↓0+y↓1×α+...+y↓(n-1)×α↑(n-1))

+x↓1×α×(y↓0+y↓1×α+...+y↓(n-1)×α↑(n-1))

+x↓2×α↑2×(y↓0+y↓1×α+...+y↓(n-1)×α↑(n-1))

...

+x↓(n-1)×α↑(n-1)×(y↓0+y↓1×α+...+y↓(n-1)×α↑(n-1))

であり、

α↑n=β mod f(g)

であるので、

$x \times I = x\downarrow 0 \times (y\downarrow 0 + y\downarrow 1 \times \alpha + \ldots + y\downarrow (n-1) \times \alpha \uparrow (n-1))$

$+ x\downarrow 1 \times (y\downarrow 0 \times \alpha + y\downarrow 1 \times \alpha \uparrow 2 + \ldots + y\downarrow (n-1) \times \beta)$

$+ x\downarrow 2 \times (y\downarrow 0 \times \alpha \uparrow 2 + y\downarrow 1 \times \alpha \uparrow 3 + \ldots + y\downarrow (n-1) \times \alpha \times \beta)$

$\ldots$

$+ x\downarrow (n-1) \times (y\downarrow 0 \times \alpha \uparrow (n-1) + y\downarrow 1 \times \beta + \ldots + y\downarrow (n-1) \times \alpha \uparrow (n-2)\beta)$

であり、αの降冪の順に整理すると

$x \times I = x\downarrow 0 \times y\downarrow 0 + \beta \times x\downarrow (n-1) \times y\downarrow 1 + \ldots + \beta \times x\downarrow 1 \times y\downarrow (n-1)$

$+ \alpha \times (x\downarrow 1 \times y\downarrow 0 + x\downarrow 0 \times y\downarrow 1 + \ldots + \beta \times x\downarrow 2 \times y\downarrow (n-1))$

$+ \alpha \uparrow 2 \times (x\downarrow 2 \times y\downarrow 0 + x\downarrow 1 \times y\downarrow 1 + \ldots + \beta \times x\downarrow 3 \times y\downarrow (n-1))$

$\ldots$

$+ \alpha \uparrow (n-1) \times (x\downarrow (n-1) \times y\downarrow 0 + x\downarrow (n-2) \times y\downarrow 1 + \ldots + x\downarrow 0 \times y\downarrow (n-1))$

である。これが1に等しいので、上記例の方程式生成部401によって生成された方程式が導くことができる。したがって、拡大体GF(q)の逆元を求めることは、基礎体GF(p)上の連立方程式を解くことと等しい。

【００２４】

また、上記例では、$g \uparrow n-\beta$の形の生成多項式を扱ったが、一般の生成多項式に対しても同様の操作により、方程式を生成できる。

【００２５】

(従来例３)

以下で、従来の基礎体GF(p)上の連立方程式の解法について図８を用いて説明する。この解法は、ガウスの消去法と呼ばれる。ガウスの消去法については、水上孝一編著、"コンピュータによる数値計算"、プログラミング入門シリーズ、朝倉書店、1985、76～82ページに詳しく述べられている。

【００２６】

$x\downarrow k (1 \leqq k \leqq n)$に対する連立方程式を、

$a\downarrow (11) \times x\downarrow 1 + a\downarrow (12) \times x\downarrow 2 + \ldots + a\downarrow (1n) \times x\downarrow n = b\downarrow 1$

$a\downarrow (21) \times x\downarrow 1 + a\downarrow (22) \times x\downarrow 2 + \ldots + a\downarrow (2n) \times x\downarrow n = b\downarrow 2$

$\ldots$

a↓(n1)×x↓1+a↓(n2)×x↓2+...+a↓(nn)×x↓n=b↓n

とし、この解を求める。

【００２７】

step1:第１方程式変換部501

行列M、ベクトルz、vを以下のようにおく。

【００２８】

M=(a↓(ij)を第i行第j列の成分とする行列)

v=(b↓kを第k行の成分とする縦ベクトル)

step2:第２方程式変換部502

行列Mを三角化するように方程式、すなわち、行列M、vを変換する。

【００２９】

step3:方程式求解部503

第２方程式変換部502によって変換された行列M、ベクトルvを用いて、方程式の解を求める。

【００３０】

上記例の第１方程式変換部501において、ベクトルXを

X=(x↓kを第k行の成分とする縦ベクトル)

とするとき、

M・X=v

が成り立つ。ただし、・は行列とベクトルの乗算である。第１方程式変換部501は、このように方程式を上式のような行列で表せる式に変換していることになる。

【００３１】

第２方程式変換部502では、方程式の解を変化しない変換により、行列を上三角行列に変換する。このとき、この上三角行列の対角成分は1である。詳しくは上記文献を参照していただきたい。対角成分を1にするため、基礎体の逆元演算がn回と乗算が1/2×n×(n-1)回必要になる。その他、行列の下三角を0にするために、基礎体の乗算が1/3×n×(n-1)×(n+1)回必要になる。基礎体の乗算、逆元演算の計算量をそれぞれ、Mul、Invとするとき、第２方程式変換部502の計算量

は、

1/6×n×(2×n↑2+3×n-5)×Mul+n×Inv

である。

【００３２】

方程式求解部503は、第２方程式変換部502で行列が対角成分1の上三角行列に変換されているため、x↓nからx↓1まで順番に簡単な計算で解を求めることができる。この計算量は、1/2×n×(n+1)×Mulである。

【００３３】

以上より、従来例３の全計算量は、

1/3×n×(n↑2+3×n-1)×Mul+n×Inv

である。このように基礎体の逆元演算が多くなる。一般に基礎体の逆元演算は計算量が大きいため、従来例３の全体の計算量が大きくなるという問題がある。

【００３４】

【発明が解決しようとする課題】

暗号システムにおいて、高速な有限体上の連立方程式の求解及び、拡大体上の逆元演算を実現することは重要である。従来技術である有限体上の連立方程式の求解法においては、基礎体の逆元演算の計算量が大きいという欠点がある。

【００３５】

本発明は、以上の従来技術における問題点を鑑みて行われたもので、基礎体の逆元演算の回数を削減することにより、有限体上の連立方程式の求解及び、拡大体上の逆元演算の計算時間を短縮し、これにより高速な暗号方式、署名方式を提供することを目的とする。

【００３６】

【課題を解決するための手段】

請求項１における発明は、予め与えられた有限体GF(p)(p:素数)において、正の整数nと、GF(p)上のn元連立一次方程式のパラメータa↓(ij)(1≦i、j≦n)、b↓k(1≦k≦n)を入力とし、前記方程式の解を出力する有限体上の演算装置であって、前記連立方程式を行列と第１のベクトルで表現し、前記行列と前記第１のベクトルを出力する第１方程式変換部と、前記第１方程式変換部から出力される前

記行列を三角化変換するために、前記行列と前記第１のベクトルを変換し、変換された三角行列と第２のベクトルを出力する第２方程式変換部と、前記第２方程式変換部から出力される前記三角行列の対角成分のGF(p)上の逆元を出力する逆元演算部と、前記第２方程式変換部から出力される三角行列と前記第２のベクトルと、前記逆元演算部から出力される逆元を用いて前記n元連立一次方程式の解を求める方程式求解部を備え、前記第２方程式変換部では、前記有限体の逆元演算を行わないことを特徴とする。

【００３７】

請求項２における発明は、請求項１の逆元演算部は、前記第２方程式変換部から出力される三角行列の対角成分をm↓1、m↓2、...、m↓nとし、出力するGF(p)上の逆元をI↓1、...、I↓nとするとき、t↓i=Π↓(k≠i) m↓k mod p (i=1、2、...、n)とt=Π↓k m↓k mod pを計算する乗算手段と、u=1/t mod pを計算する第１逆元演算手段と、I↓i = u×t↓i mod p (i=1、2、...、n)を計算する第２逆元演算手段からなることを特徴とする(ただし、x↓1はxの下付き添字が1であることを示す)。

【００３８】

請求項３における発明は、請求項２の乗算手段は、前記t↓i(i=1、2、...、n)をs↓1=m↓1×m↓2 mod p、s↓2=s↓1×m↓3 mod p、...、s↓(n-3)=s↓(n-4)×m↓(n-2) mod p、t↓n=s↓(n-3)×m↓(n-1) mod p、t↓(n-1)=s↓(n-3)×m↓n mod p、s↓n=m↓(n-1)×m↓n mod p、t↓(n-2)=s↓(n-4)×s↓n mod p、s↓(n-1)=m↓(n-2)×s↓n mod p、t↓(n-3)=s↓(n-5)×s↓(n-1) mod p、s↓(n-2)=m↓(n-3)×s↓(n-1) mod p、t↓(n-4)=s↓(n-6)×s↓(n-2) mod p、...、s↓5=m↓4×s↓6 mod p、t↓3=s↓1×s↓5 mod p、s↓4=m↓3×s↓5 mod p、t↓2=m↓1×s↓4 mod p、t↓1=m↓2×s↓4 mod pにより計算し、tを予め与えられたkを用いて、t=t↓k×m↓kにより計算することを特徴とする。

【００３９】

請求項４における発明は、予め与えられた有限体GF(p)の拡大体GF(q)(q=p↑n)において、GF(q)の元xを入力とし、xのGF(q)上の逆元を出力する逆元演算装置であって、前記元xを入力とし、前記元xの逆元を求めるための連立方程式を生成す

る方程式生成部と、前記方程式生成部から出力される連立方程式の解を求める方程式計算部と、前記方程式計算部の解をxの逆元に変換する逆元変換部を備え、前記方程式計算部は請求項１記載の有限体上の演算装置であることを特徴とする(ただし、p↑nはpのn乗を示す)。

【００４０】

請求項５における発明は、予め与えられた有限体GF(p)の拡大体GF(q)(q=p↑n)において、GF(q)の元xを入力とし、xのGF(q)上の逆元を出力する逆元演算装置であって、前記元xを入力とし、前記元xの逆元を求めるための連立方程式を生成する方程式生成部と、前記方程式生成部から出力される連立方程式の解を求める方程式計算部と、前記方程式計算部の解をxの逆元に変換する逆元変換部を備え、前記方程式計算部は請求項２記載の有限体上の演算装置であることを特徴とする。

【００４１】

請求項６における発明は、予め与えられた有限体GF(p)の拡大体GF(q)(q=p↑n)において、GF(q)の元xを入力とし、xのGF(q)上の逆元を出力する逆元演算装置であって、前記元xを入力とし、前記元xの逆元を求めるための連立方程式を生成する方程式生成部と、前記方程式生成部から出力される連立方程式の解を求める方程式計算部と、前記方程式計算部の解をxの逆元に変換する逆元変換部を備え、前記方程式計算部は請求項３記載の有限体上の演算装置であることを特徴とする。

【００４２】

請求項７における発明は、予め与えられた有限体GF(p)を利用する有限体利用暗号システムであって、有限体上の暗号装置と、正の整数nとGF(p)上のn元連立一次方程式のパラメータa↓(ij)(1≦i、j≦n)、b↓k(1≦k≦n)を入力とし、前記方程式の解を出力する連立方程式求解装置を備え、前記連立方程式求解装置は請求項１記載の有限体上の演算装置であることを特徴とする。

【００４３】

請求項８における発明は、予め与えられた有限体GF(p)を利用する有限体利用暗号システムであって、有限体を上の暗号装置と、正の整数nとGF(p)上のn元連

立一次方程式のパラメータa↓(ij)(1≦i、j≦n)、b↓k(1≦k≦n)を入力とし、前記方程式の解を出力する連立方程式求解装置を備え、前記連立方程式求解装置は請求項２記載の有限体上の演算装置であることを特徴とする。

【００４４】

請求項９における発明は、予め与えられた有限体GF(p)を利用する有限体利用暗号システムであって、有限体上の暗号装置と、正の整数nとGF(p)上のn元連立一次方程式のパラメータa↓(ij)(1≦i、j≦n)、b↓k(1≦k≦n)を入力とし、前記方程式の解を出力する連立方程式求解装置を備え、前記連立方程式求解装置は請求項３記載の有限体上の演算装置であることを特徴とする。

【００４５】

請求項１０における発明は、予め与えられた有限体GF(p)の拡大体GF(q)(q=p↑n)を利用する拡大体利用暗号システムであって、拡大体上の暗号装置と、GF(q)の元xを入力とし、xのGF(q)上の逆元を出力する逆元演算装置を備え、前記逆元演算装置は請求項４記載の逆元演算装置であることを特徴とする。

【００４６】

請求項１１における発明は、予め与えられた有限体GF(p)の拡大体GF(q)(q=p↑n)を利用する拡大体利用暗号システムであって、拡大体上の暗号装置と、GF(q)の元xを入力とし、xのGF(q)上の逆元を出力する逆元演算装置を備え、前記逆元演算装置は請求項５記載の逆元演算装置であることを特徴とする。

【００４７】

請求項１２における発明は、予め与えられた有限体GF(p)の拡大体GF(q)(q=p↑n)を利用する拡大体利用暗号システムであって、拡大体上の暗号装置と、GF(q)の元xを入力とし、xのGF(q)上の逆元を出力する逆元演算装置を備え、前記逆元演算装置は請求項６記載の逆元演算装置であることを特徴とする。

【００４８】

【発明の実施の形態】

(実施形態１)

図１は、実施形態１における有限体上の演算装置の構成を示すブロック図である。

【００４９】

この有限体上の演算装置は、予め与えられた体GF(p)(p:素数)において、正の整数nと以下のn元連立一次方程式のパラメータa↓(ij)(1≦i、j≦n)、b↓k(1≦k≦n)を与えられたとき、前記方程式のGF(p)上の解を出力するものである。

【００５０】

a↓(11)×x↓1+a↓(12)×x↓2+...+a↓(1n)×x↓n=b↓1

a↓(21)×x↓1+a↓(22)×x↓2+...+a↓(2n)×x↓n=b↓2

...

a↓(n1)×x↓1+a↓(n2)×x↓2+...+a↓(nn)×x↓n=b↓n

有限体上の演算装置10は、第１方程式変換部101と、第２方程式変換部102と、逆元演算部103と、方程式求解部104を備える。

【００５１】

第１方程式変換部101は、nとa↓(ij)(1≦i、j≦n)、b↓k(1≦k≦n)を入力とし、それらの方程式のパラメータを以下の行列M[1]とベクトルv[1]に変換し、出力する。

【００５２】

M[1]=(a↓(ij)を第i行第j列の成分とする行列)

v[1]=(b↓kを第k行の成分とする縦ベクトル)

第２方程式変換部102は、第１方程式変換部101から出力された行列M[1]とベクトルv[1]を行列M[1]が三角化されるように変換し、変換された行列M[2]とベクトルv[2]を出力する。

【００５３】

逆元演算部103は、第２方程式変換部102から出力された行列M[2]の対角成分m↓k(1≦k≦n)のGF(p)上の逆元I↓kを計算し、出力する。

【００５４】

方程式求解部104は、第２方程式変換部102から出力された行列M[2]とベクトルv[2]と逆元演算部103から出力された逆元I↓k(1≦k≦n)を用いて、方程式の解を求め出力する。

【００５５】

（第１方程式変換部101の検証）

ベクトルx[1]を以下のように定義する。

【００５６】

x[1]=(x↓kを第k行の成分とする縦ベクトル)

このとき、

M[1]・x[1]=v[1]

が成り立つ。ただし、・は行列とベクトルの乗算である。第１方程式変換部101は、このように方程式を上式のような行列で表せる式に変換していることになる。

【００５７】

（第２方程式変換部102の構成）

図２は、第２方程式変換部102の構成を示すブロック図である。

【００５８】

第２方程式変換部102は、第１方程式変換部101から出力された行列M[1]とベクトルv[1]を行列が三角化されるように変換し、変換された行列M[2]とベクトルv[2]を出力する方程式変換装置である。

【００５９】

第２方程式変換部102は、第１初期値設定部1021と、探索部1022と、第２初期値設定部1023と、三角化部1024と、第１終了判定部1025と、第２終了判定部1026を備える。

【００６０】

第１初期値設定部1021は、カウンタjを1に設定する。

【００６１】

探索部1022は、第j列の成分の中でGF(p)上で0でない成分を第j行から第n行まで探索し、はじめに発見した成分の行数をkとする。さらにk≠jの場合に、行列M[2]、v[2]のそれぞれの第k行と第j行を入れ換え、行列M(j、i、2)、v(j、i、2)とし、出力する。

【００６２】

第２初期値設定部1023は、カウンタiをj+1に設定する。

【００６３】

三角化部1024は、M↓(jj)(M↓(ij)は行列M(j、i、2)のi行j列成分)とM↓(ij)を用いて、j+1≦k≦nに対して、

M↓(ij)←0

M↓(ik)←M↓(jj)×M↓(ik)-M↓(ij)×M↓(jk)

b↓i←M↓(jj)×b↓i-M↓(ij)×b↓j

のように設定し、設定後の行列をM(j、i、3)、ベクトルをv(j、i、3)とし、出力する。

【００６４】

第１終了判定部1025は、i=nであるか判定する。

【００６５】

第２終了判定部1026は、j=nであるか判定する。

【００６６】

以下に、第２方程式変換部102の動作を示す。

【００６７】

第１初期値設定部1021は、カウンタjを1に設定し、探索部1022にj、第１方程式変換部101で出力された行列M[1]、ベクトルv[1]を入力する。探索部1022は、第j列の成分の中でGF(p)上で0でない成分をj行、j+1行、...、n行まで探索し、はじめて発見した成分の行数をkとする。さらにk≠jの場合に、行列M[1]、ベクトルv[1]のそれぞれの第k行と第j行を入れ換え、入れ換えた後の行列、ベクトルをそれぞれ、M(j、i、2)、v(j、i、2)とし、第２初期値設定部1023にjを入力する。第２初期値設定部1023は、iをj+1に設定し、三角化部1024にM(j、i、2)、v(j、i、2)を入力する。三角化部1024は、M(j、i、2)、v(j、i、2)を変換し、変換後の行列、ベクトルをそれぞれ、M(j、i、3)、v(j、i、3)とし、第１終了判定部1025にiを入力する。第１終了判定部1025は、i=nであるか判定し、i=nであるとき、第２終了判定部1026にjを入力する。それ以外は、iをi+1に設定し、三角化部1024にM(j、i-1、3)、v(j、i-1、3)を入力する。第２終了判定部1026は、j=nであるか判定し、j=nであるとき、M(j、i-1、3)、v(j、i-1、3)をM[2]、v[2]として出力し、終了。それ以外は、jをj+1に設定し、探索部1022にj、M(j-1、i-1

、3)、v(j-1、i-1、3)を入力する。

【００６８】

（第２方程式変換部102の検証）

第２方程式変換部102は、行列を上三角行列になるように変換している。方程式の解を変化させないようにするため、ベクトルも変化させている。従来法と異なる点は、対角成分を1にしないことである。

【００６９】

三角化部1024の入力を行列M↓(in)、ベクトルv↓(in)とし、出力を行列M↓(out)、ベクトルv↓(out)とする。三角化部1024は、行列M↓(in)の第i、j行の行ベクトルをそれぞれ、l↓i、l↓jとするとき、

M↓(jj)×l↓i-M↓(ij)×l↓j

の計算を行い、この結果の行ベクトルをM↓(out)の第i行とし、

M↓(jj)×b↓i-M↓(ij)×b↓j

の計算を行い、v↓(out)の第i行としている。他のM↓(out)、v↓(out)の成分はM↓(in)、v↓(in)と同じである。このとき、方程式

M↓(in)・x[1]=v↓(in)

と方程式

M↓(out)・x[1]=v↓(out)

が同じ解をもつことは、以下の文献から明らかである。

【００７０】

水上孝一編著、"コンピュータによる数値計算"、プログラミング入門シリーズ、朝倉書店、1985、76～82ページ

以上より、第２方程式変換部102の方程式変換によって、解は変化しない。

【００７１】

また、三角化部1024にあるようにカウンタjに対して、j+1≦i≦nを満たすiに対して、M↓(ij)が0になる。この操作をjが1からnまで繰り返すので、行列の下三角部分が0になる。したがって、第２方程式変換部102は方程式の解を変化させずに、行列の三角化変換が行える。

【００７２】

（逆元演算部103の構成）

図３は、逆元演算部103の構成を示すブロック図である。

【００７３】

逆元演算部103は、第２方程式変換部102から出力された行列の対角成分m↓k(1≦k≦n)のGF(p)上の逆元を計算し、出力する逆元演算装置である。

【００７４】

逆元演算部103は、乗算部1031と、第１逆元演算部1032と、第２逆元演算部1033を備える。

【００７５】

乗算部1031は、

$t\downarrow i=\Pi\downarrow(k\neq i)\ m\downarrow k \bmod p \qquad (i=1、2、\ldots、n)$

を

$s\downarrow 1=m\downarrow 1\times m\downarrow 2 \bmod p$

$s\downarrow 2=s\downarrow 1\times m\downarrow 3 \bmod p$

...

$s\downarrow(n-3)=s\downarrow(n-4)\times m\downarrow(n-2) \bmod p$

$t\downarrow n=s\downarrow(n-3)\times m\downarrow(n-1) \bmod p$

$t\downarrow(n-1)=s\downarrow(n-3)\times m\downarrow n \bmod p$

$s\downarrow n=m\downarrow(n-1)\times m\downarrow n \bmod p$、$t\downarrow(n-2)=s\downarrow(n-4)\times s\downarrow n \bmod p$

$s\downarrow(n-1)=m\downarrow(n-2)\times s\downarrow n \bmod p$、$t\downarrow(n-3)=s\downarrow(n-5)\times s\downarrow(n-1) \bmod p$

$s\downarrow(n-2)=m\downarrow(n-3)\times s\downarrow(n-1) \bmod p$、$t\downarrow(n-4)=s\downarrow(n-6)\times s\downarrow(n-2) \bmod p$

...

$s\downarrow 5=m\downarrow 4\times s\downarrow 6 \bmod p$、$t\downarrow 3=s\downarrow 1\times s\downarrow 5 \bmod p$

$s\downarrow 4=m\downarrow 3\times s\downarrow 5 \bmod p$、$t\downarrow 2=m\downarrow 1\times s\downarrow 4 \bmod p$

$t\downarrow 1=m\downarrow 2\times s\downarrow 4 \bmod p$

のように求め、

$t=\Pi\downarrow k\ m\downarrow k \bmod p$

を予め与えられたkを用いて、

$t=t\downarrow k\times m\downarrow k \bmod p$

のように求める。

【００７６】

第１逆元演算部1032は、

$u=1/t \bmod p$

を計算する。

【００７７】

第２逆元演算部1033は、

$I\downarrow i=u\times t\downarrow i \bmod p \qquad (i=1、2、\ldots、n)$

を計算する。

【００７８】

以下に逆元演算部103の動作を示す。

【００７９】

乗算部1031は、$t\downarrow i=\Pi\downarrow(k\neq i)\ m\downarrow k \bmod p\ (1\leqq i\leqq n)$と、$t=\Pi\downarrow k\ m\downarrow k \bmod p$を計算し、第１逆元演算部1032にtを入力する。第１逆元演算部1032は、tのGF(p)上の逆元を計算し、それをuとし、u、$t\downarrow i(1\leqq i\leqq n)$を第２逆元演算部1033に入力する。第２逆元演算部1033は、$m\downarrow i(1\leqq i\leqq n)$のGF(p)上の逆元$I\downarrow i$を計算し、出力する。

【００８０】

(逆元演算部103の動作の検証)

乗算部1031では、

$s\downarrow 1=m\downarrow 1\times m\downarrow 2 \bmod p$

$s\downarrow 2=s\downarrow 1\times m\downarrow 3=m\downarrow 1\times m\downarrow 2\times m\downarrow 3 \bmod p$

$s\downarrow 3=s\downarrow 2\times m\downarrow 4=m\downarrow 1\times m\downarrow 2\times m\downarrow 3\times m\downarrow 4 \bmod p$

...

$s\downarrow(n-3)=m\downarrow 1\times m\downarrow 2\times m\downarrow 3\times\ldots\times m\downarrow(n-2) \bmod p$

$t\downarrow n=s\downarrow(n-3)\times m\downarrow(n-1)=m\downarrow 1\times m\downarrow 2\times m\downarrow 3\times\ldots\times m\downarrow(n-1)=\Pi\downarrow(k\neq n)\ m\downarrow k \bmod p$

で、$t\downarrow n$を求める。

【００８１】

t↓(n-1)=s↓(n-3)×m↓n=m↓1×m↓2×m↓3×...×m↓(n-2)×m↓n=Π↓(k≠n-1) m↓k mod p

で、t↓(n-1)を計算し、

s↓n=m↓(n-1)×m↓n= mod p

t↓(n-2)=s↓(n-4)×s↓n=m↓1×m↓2×m↓3×...×m↓(n-3)×m↓(n-1)×m↓n=Π↓(k≠n-2) m↓k mod p

で、t↓(n-2)を計算する。

【００８２】

以下、同様にして、

t↓(n-3)からt↓2まで計算する。

【００８３】

さらに、

t↓1=m↓2×s↓4=m↓2×m↓3×...×m↓n=Π↓(k≠1) m↓k mod p

で、t↓1を求め、これまでに求めたt↓k(1≦k≦n)のいずれかを用いて、

t=t↓k×m↓k mod p

を計算する。

【００８４】

第１逆元演算部1032で、tの逆元uを求める。

【００８５】

第２逆元演算部1033では、

u=1/(m↓1×m↓2×m↓3×...×m↓n) mod p

であり、t↓i=Π↓(k≠i) m↓k mod p (1≦i≦n)であるので、

1/m↓i=u×t↓i mod p

が成り立つことを利用して、m↓iの逆元I↓iを求める。以上より、すべてのm↓i(1≦i≦n)の逆元I↓iが得られる。

【００８６】

(方程式求解部104の構成)

図４は、方程式求解部104の構成を示すブロック図である。

【００８７】

方程式求解部104は、第２方程式変換部102から出力された行列M[2]とベクトルv[2]と逆元演算部103から出力された逆元I↓i(1≦i≦n)を用いて、方程式の解を求め出力する。以下では、解をy↓iとする。

【００８８】

方程式求解部104は、初期値設定部1041と、求解部1042と、終了判定部1043を備える。

【００８９】

初期値設定部1041は、カウンタcをnに設定する。

【００９０】

求解部1042は、y↓c を次のように計算する。

【００９１】

$y\downarrow c=I\downarrow c\times b\downarrow c-\Sigma\downarrow(c+1\leqq i\leqq n)\ (M\downarrow(ci)\times y\downarrow i)$

ここで、M↓(ij)は、行列M[2]の第i行第j列成分であり、b↓iはベクトルv[2]の第i行成分である。

【００９２】

終了判定部1043は、c=0であるか判定する。

【００９３】

以下に方程式求解部104の動作を示す。

【００９４】

初期値設定部1041は、cをnに設定し、求解部1042にcと第２方程式変換部102から出力されたM[2]、v[2]と逆元演算部103から出力されたI↓cを入力する。求解部1042は、y↓cを求め、終了判定部1043にcを入力する。終了判定部1043は、c=0であるか判定し、c=0であるとき、解y↓k(1≦k≦n)を出力する。それ以外は、cをc+1に設定し、求解部1042にM[2]、v[2]、I↓cを入力する。

【００９５】

(方程式求解部104の検証)

第２方程式変換102から出力された行列M[2]は上三角化行列であるので、方程式

$M[2]\cdot x[1]=v[2]$

は、

$$M\downarrow(11)\times x\downarrow 1+M\downarrow(12)\times x\downarrow 2+M\downarrow(13)\times x\downarrow 3+\ldots+M\downarrow(1n)\times x\downarrow n=b\downarrow 1$$

$$M\downarrow(22)\times x\downarrow 2+M\downarrow(23)\times x\downarrow 3+\ldots+M\downarrow(2n)\times x\downarrow n=b\downarrow 2$$

$\ldots$

$$M\downarrow(nn)\times x\downarrow n=b\downarrow n$$

の形をしている。また、行列の対角成分の逆元を求めているので、$x\downarrow n$の解$y\downarrow n$は、

$$y\downarrow n=I\downarrow n\times b\downarrow n \bmod p$$

であり、$x\downarrow(n-1)$の解$y\downarrow(n-1)$は、

$$y\downarrow(n-1)=I\downarrow(n-1)\times b\downarrow(n-1)-M\downarrow(n-1,\ n)\times y\downarrow n$$

である。同様にして、$x\downarrow c$の解$y\downarrow c$は、

$$y\downarrow c=I\downarrow c\times b\downarrow c-\Sigma\downarrow(c+1\leqq i\leqq n)\ (M\downarrow(ci)\times y\downarrow i)$$

である。

【００９６】

以上の各部の検証より、本実施形態１の有限体上の演算装置は、有限体上の連立方程式の解を求めることができる。

【００９７】

（実施形態１の効果）

この例の計算量について説明する。以下で、従来の方法との比較を行う。

【００９８】

基礎体GF(p)の乗算、逆元演算の計算量をそれぞれ、Mul、Invとする。従来の方法では、従来例３に示すような方法を用いて連立方程式の解を求めていた。この場合、計算量は$1/3\times n\times(n\uparrow 2+3\times n-1)\times Mul+n\times Inv$である。本実施形態１では、三角化部102の計算量が、$2/3\times n\times(n-1)\times(n+1)\times Mul$であり、逆元演算部の計算量が$(4\times n-5)\times Mul+Inv$、方程式求解部104の計算量が$1/2\times n\times(n+1)\times Mul$であるので、逆元演算装置10全体の計算量は、$(2/3\times n\uparrow 3+1/2\times n\uparrow 2+23/6\times n-5)\times Mul+Inv$である。$n=5$、$|q|=160$（$|q|$はqのビットサイズ）の場合、一般的な計算機では、$Inv=40Mul$であることが知られているので、従来法の計算量が、$265\times Mul$であり、本実施形態１では、$150\times Mul$である。したがって、連立方程式求解が

高速な有限体上の演算装置を提供することができ、この実用的価値は非常に大きい。なお、本実施形態１を用いた暗号システム並びに、誤り訂正システムが実現可能となる。

【００９９】

（実施形態２）

図５は、実施形態２における逆元演算装置の構成を示すブロック図である。

【０１００】

この逆元演算装置は、予め与えられた有限体GF(p)の拡大体GF(q)(q=p↑n)において、GF(q)の元xを入力とし、xのGF(q)上の逆元Iを出力する。以下では、拡大体GF(q)の生成多項式をg↑n−βとし、その根をα、x=x↓0+x↓1×α+...+x↓(n−1)×α↑(n−1)とする。

【０１０１】

逆元演算装置20は、方程式生成部201と、方程式計算部202と、逆元変換部203を備える。

【０１０２】

方程式生成部201は、xから以下のy↓i(0≦i≦n−1)に関する連立方程式を生成する。

【０１０３】

$x\downarrow 0\times y\downarrow 0+\beta\times x\downarrow(n-1)\times y\downarrow 1+\beta\times x\downarrow(n-2)\times y\downarrow 2+\ldots+\beta\times x\downarrow 1\times y\downarrow(n-1)=1$

$x\downarrow 1\times y\downarrow 0+x\downarrow 0\times y\downarrow 1+\beta\times x\downarrow(n-1)\times y\downarrow 2+\ldots+\beta\times x\downarrow 2\times y\downarrow(n-1)=0$

$x\downarrow 2\times y\downarrow 0+x\downarrow 1\times y\downarrow 1+x\downarrow 0\times y\downarrow 2+\ldots+\beta\times x\downarrow 3\times y\downarrow(n-1)=0$

...

$x\downarrow(n-1)\times y\downarrow 0+x\downarrow(n-2)\times y\downarrow 1+x\downarrow(n-3)\times y\downarrow 2+\ldots+x\downarrow 0\times y\downarrow(n-1)=0$

方程式計算部202は、実施形態１の有限体の演算装置と同一である。

【０１０４】

逆元変換部203は、方程式計算部202から出力された解y↓k(1≦k≦n)を逆元Iに以下のように変換する。

【０１０５】

$I=y\downarrow 0+y\downarrow 1\times\alpha+\ldots+y\downarrow(n-1)\times\alpha\uparrow(n-1)$

以下に逆元演算装置20の動作を示す。

【０１０６】

方程式生成部201は、xとGF(q)の生成多項式から連立方程式を生成し、その方程式のパラメータを方程式計算部202に入力する。方程式計算部202は、方程式の解を求め、その解を逆元変換部203に入力する。逆元変換部203は、方程式の解を逆元に変換し、出力する。

【０１０７】

(実施形態２の検証)

本実施形態２のIとxについて、

$x\times I=1 \mod f(g)$

という関係式であるとき、

$$x\times I=x\downarrow 0\times(y\downarrow 0+y\downarrow 1\times\alpha+\ldots+y\downarrow(n-1)\times\alpha\uparrow(n-1))$$
$$+x\downarrow 1\times\alpha\times(y\downarrow 0+y\downarrow 1\times\alpha+\ldots+y\downarrow(n-1)\times\alpha\uparrow(n-1))$$
$$+x\downarrow 2\times\alpha\uparrow 2\times(y\downarrow 0+y\downarrow 1\times\alpha+\ldots+y\downarrow(n-1)\times\alpha\uparrow(n-1))$$
$$\ldots$$
$$+x\downarrow(n-1)\times\alpha\uparrow(n-1)\times(y\downarrow 0+y\downarrow 1\times\alpha+\ldots+y\downarrow(n-1)\times\alpha\uparrow(n-1))$$

であり、

$\alpha\uparrow n=\beta \mod f(g)$

であるので、

$$x\times I=x\downarrow 0\times(y\downarrow 0+y\downarrow 1\times\alpha+\ldots+y\downarrow(n-1)\times\alpha\uparrow(n-1))$$
$$+x\downarrow 1\times(y\downarrow 0\times\alpha+y\downarrow 1\times\alpha\uparrow 2+\ldots+y\downarrow(n-1)\times\beta)$$
$$+x\downarrow 2\times(y\downarrow 0\times\alpha\uparrow 2+y\downarrow 1\times\alpha\uparrow 3+\ldots+y\downarrow(n-1)\times\alpha\times\beta)$$
$$\ldots$$
$$+x\downarrow(n-1)\times(y\downarrow 0\times\alpha\uparrow(n-1)+y\downarrow 1\times\beta+\ldots+y\downarrow(n-1)\times\alpha\uparrow(n-2)\beta)$$

であり、αの降冪の順に整理すると

$$x\times I=x\downarrow 0\times y\downarrow 0+\beta\times x\downarrow(n-1)\times y\downarrow 1+\ldots+\beta\times x\downarrow 1\times y\downarrow(n-1)$$
$$+\alpha\times(x\downarrow 1\times y\downarrow 0+x\downarrow 0\times y\downarrow 1+\ldots+\beta\times x\downarrow 2\times y\downarrow(n-1))$$
$$+\alpha\uparrow 2\times(x\downarrow 2\times y\downarrow 0+x\downarrow 1\times y\downarrow 1+\ldots+\beta\times x\downarrow 3\times y\downarrow(n-1))$$

・・・

$+\alpha \uparrow (n-1)\times(x\downarrow(n-1)\times y\downarrow 0+x\downarrow(n-2)\times y\downarrow 1+\ldots+x\downarrow 0\times y\downarrow(n-1))$

である。これが1に等しいので、方程式生成部201によって生成された方程式が導くことができる。したがって、拡大体GF(q)の逆元を求めることは、基礎体GF(p)上の連立方程式を解くことと等しい。

【０１０８】

また、上記例では、$g\uparrow n-\beta$ の形の生成多項式を扱ったが、一般の生成多項式に対しても同様の操作により、方程式を生成できる。

【０１０９】

（実施形態２の効果）

この例の計算量については、実施形態１で述べたとおりである。本実施形態２によって、高速な逆元演算装置を実現可能となり、実用的価値は非常に大きい。なお、本実施形態２を用いた暗号システム並びに、誤り訂正システムが実現可能となる。

【０１１０】

【発明の効果】

以上に説明したように本発明は、従来例における問題点を鑑みて行われたもので、有限体上の連立方程式求解及び、拡大体上の逆元演算の計算時間を短縮できた。

【０１１１】

以上により、高速な暗号方式や署名方式を可能にする有限体上の演算装置及び、逆元演算装置を提供することができ，その実用的価値は大きい。

【図面の簡単な説明】

【図１】

本発明の実施形態１の有限体上の演算装置のブロック図

【図２】

本発明の実施形態１の第２方程式変換部のブロック図

【図３】

本発明の実施形態１の逆元演算部のブロック図

【図４】

本発明の実施形態１の方程式求解部のブロック図

【図５】

本発明の実施形態２の逆元演算装置のブロック図

【図６】

従来例１のエルガマル署名によるデジタル署名方式の手順を示すシーケンス図

【図７】

従来例２の逆元演算装置のブロック図

【図８】

従来例３の連立方程式の求解装置のブロック図

【符号の説明】

１０　本発明の実施形態１の有限体上の演算装置

１０１　第１方程式変換部

１０２　第２方程式変換部

１０２１　第１初期値設定部

１０２２　探索部

１０２３　第２初期値設定部

１０２４　三角化部

１０２５　第１終了判定部

１０２６　第２終了判定部

１０３　逆元演算部

１０３１　乗算部

１０３２　第１逆元演算部

１０３３　第２逆元演算部

１０４　方程式求解部

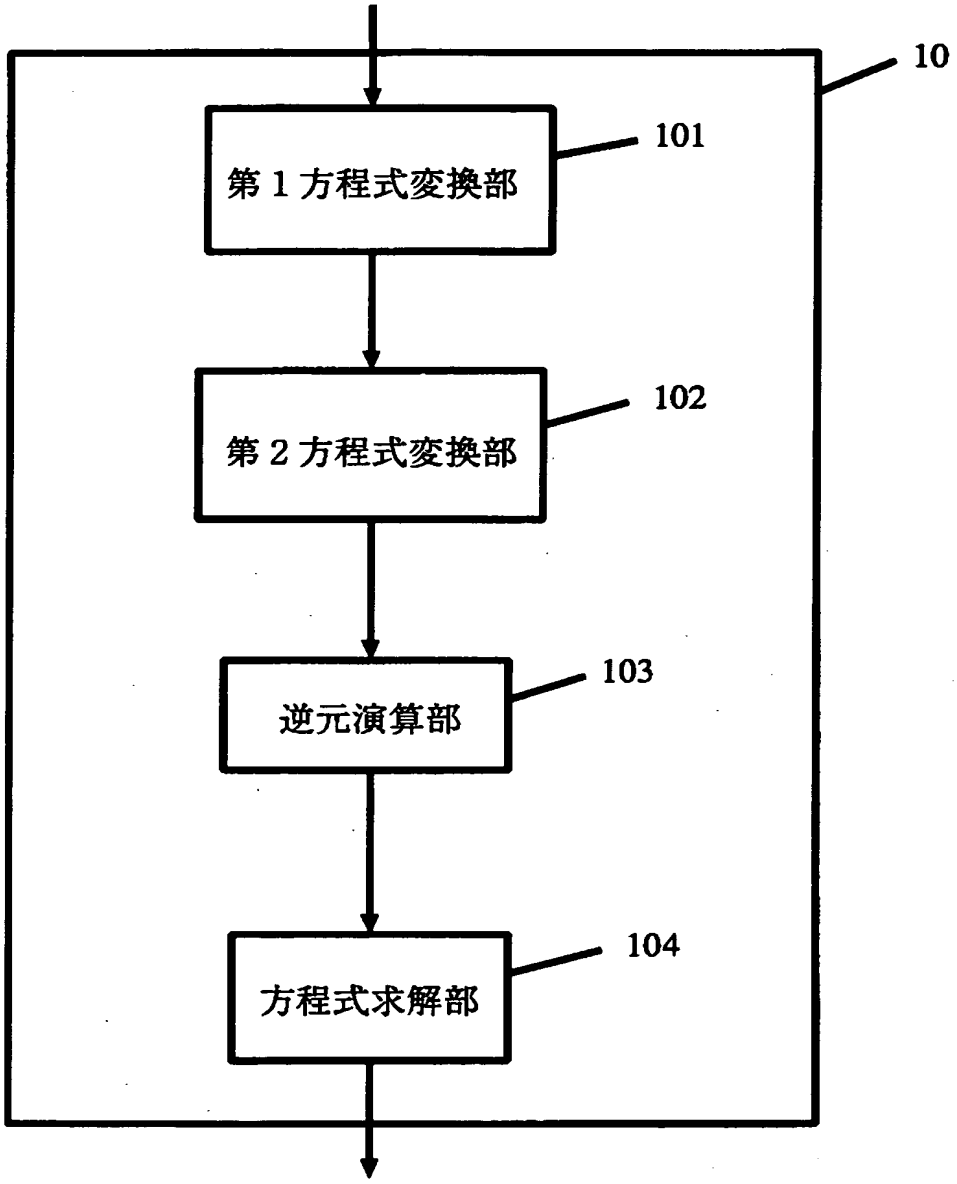
１０４１　初期値設定部

１０４２　求解部

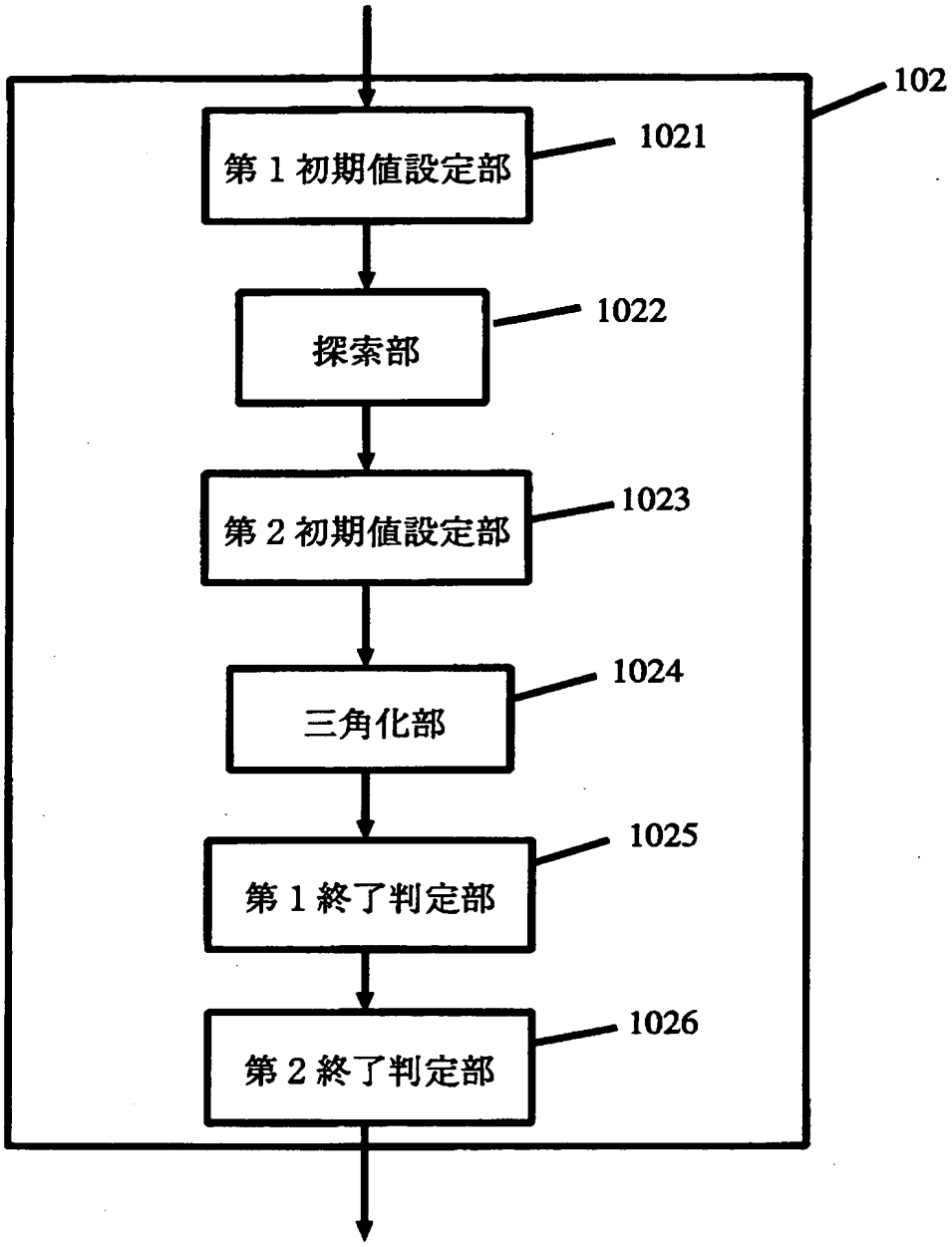
１０４３　終了判定部

【書類名】　　図面

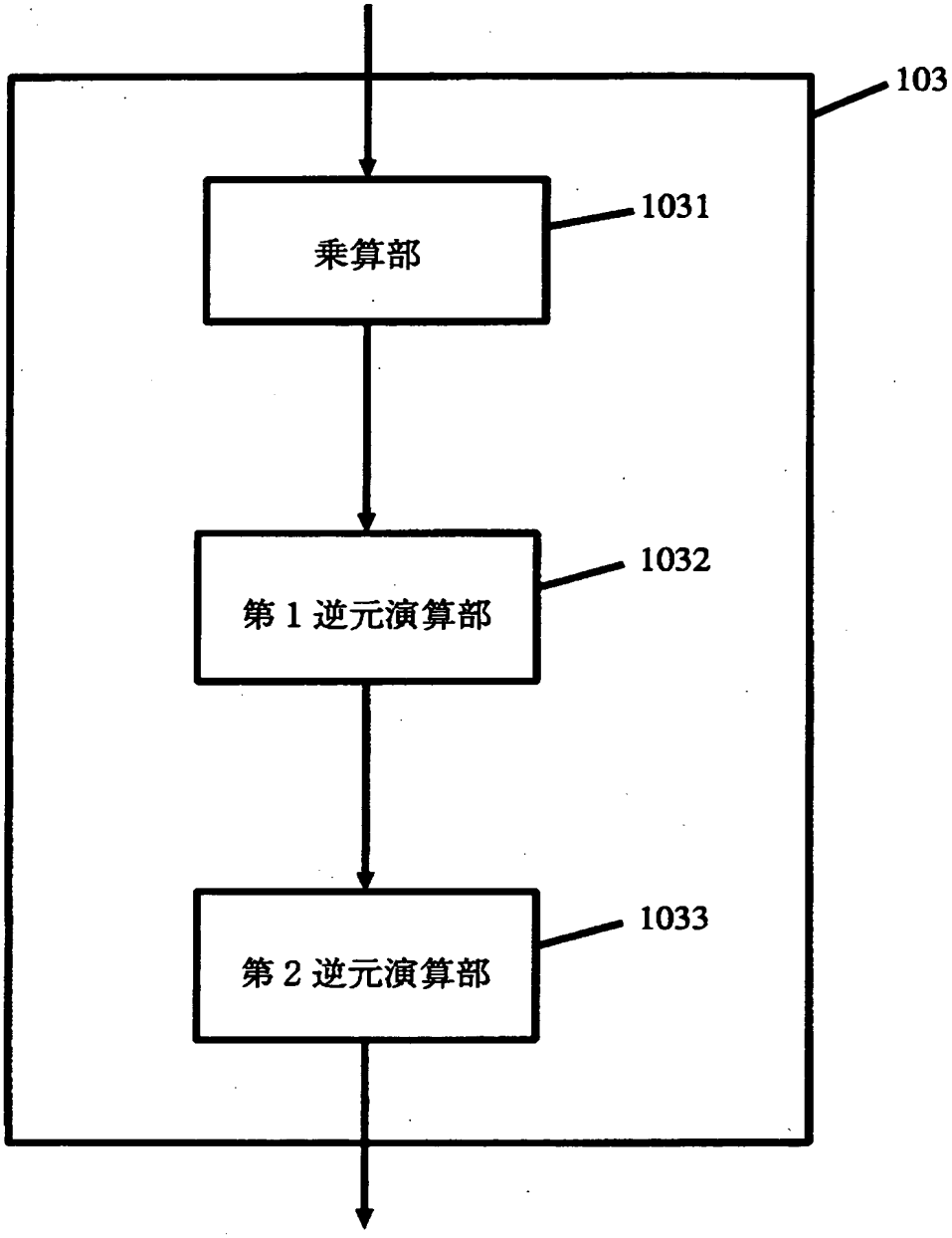
【図１】



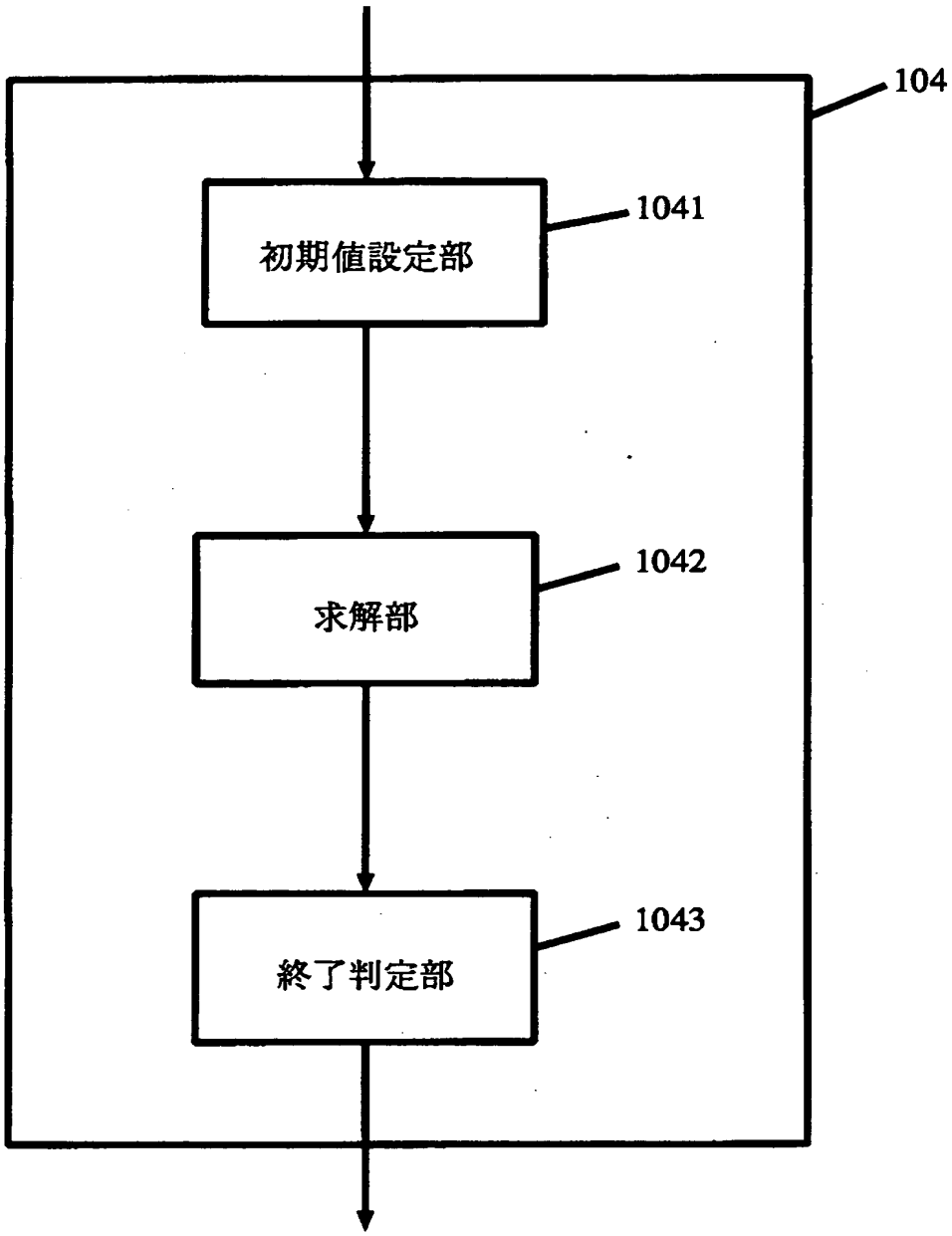
【図２】


102
第１初期値設定部
1021
探索部
1022
第２初期値設定部
1023
三角化部
1024
第１終了判定部
1025
第２終了判定部
1026

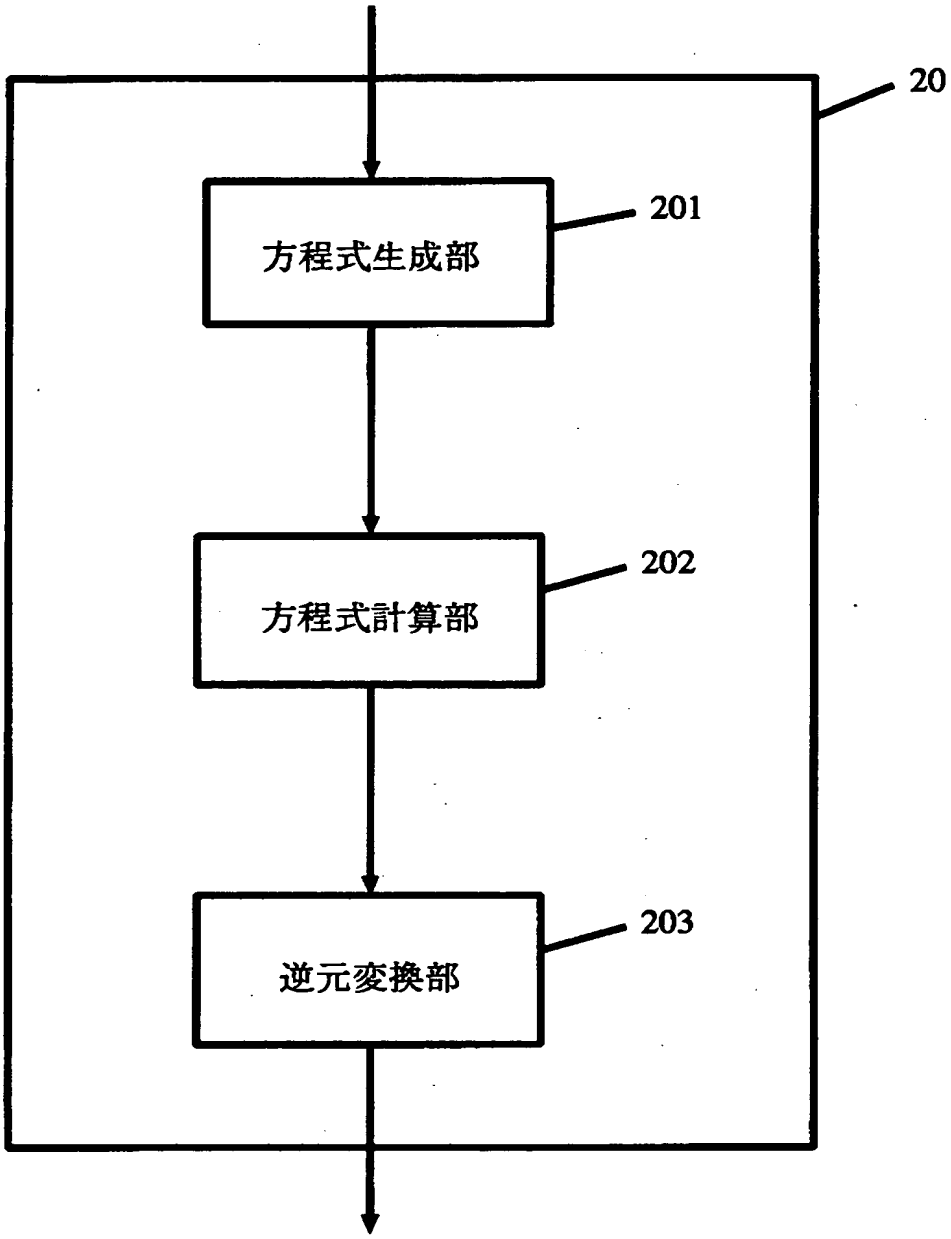
【図３】



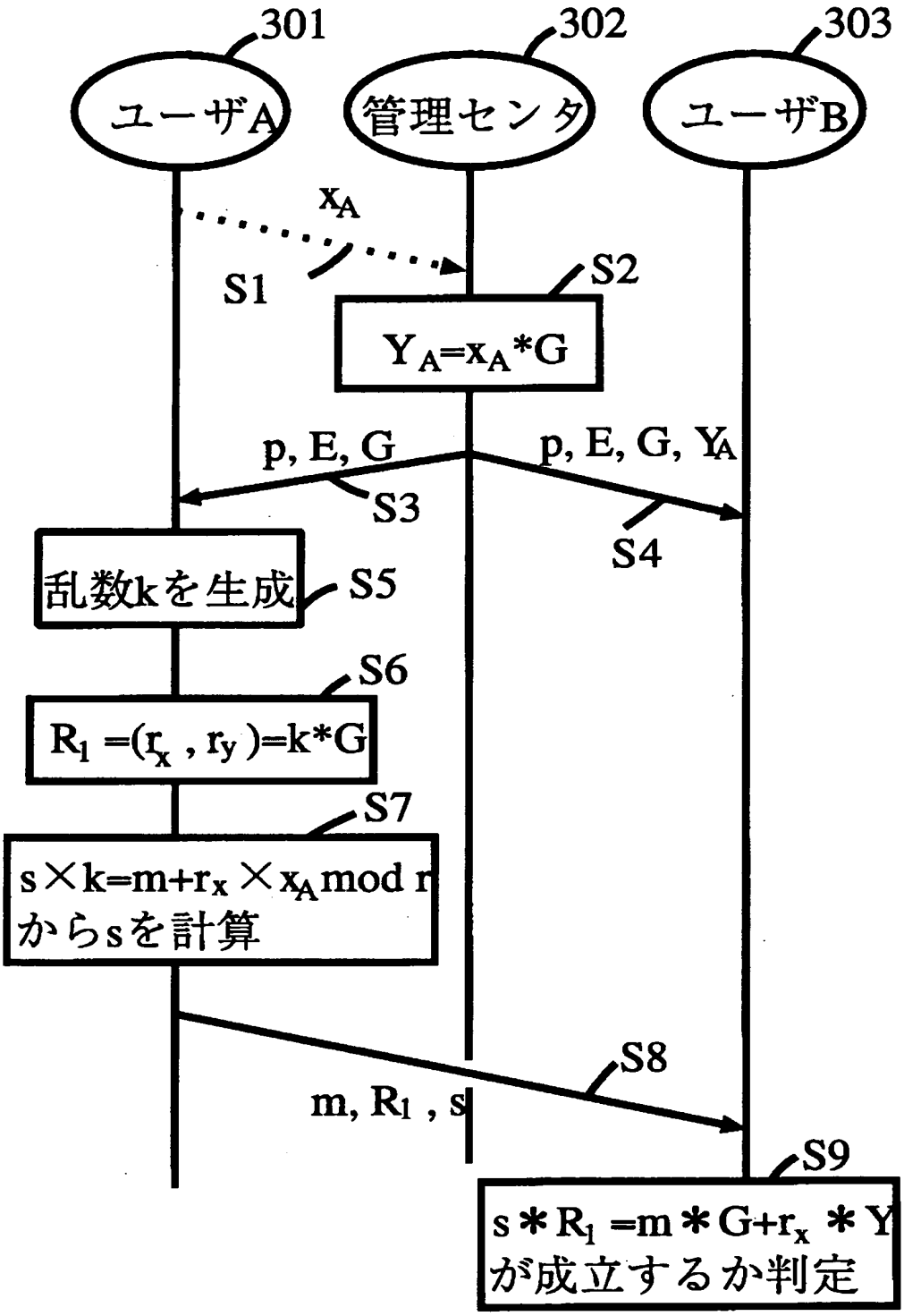
【図４】



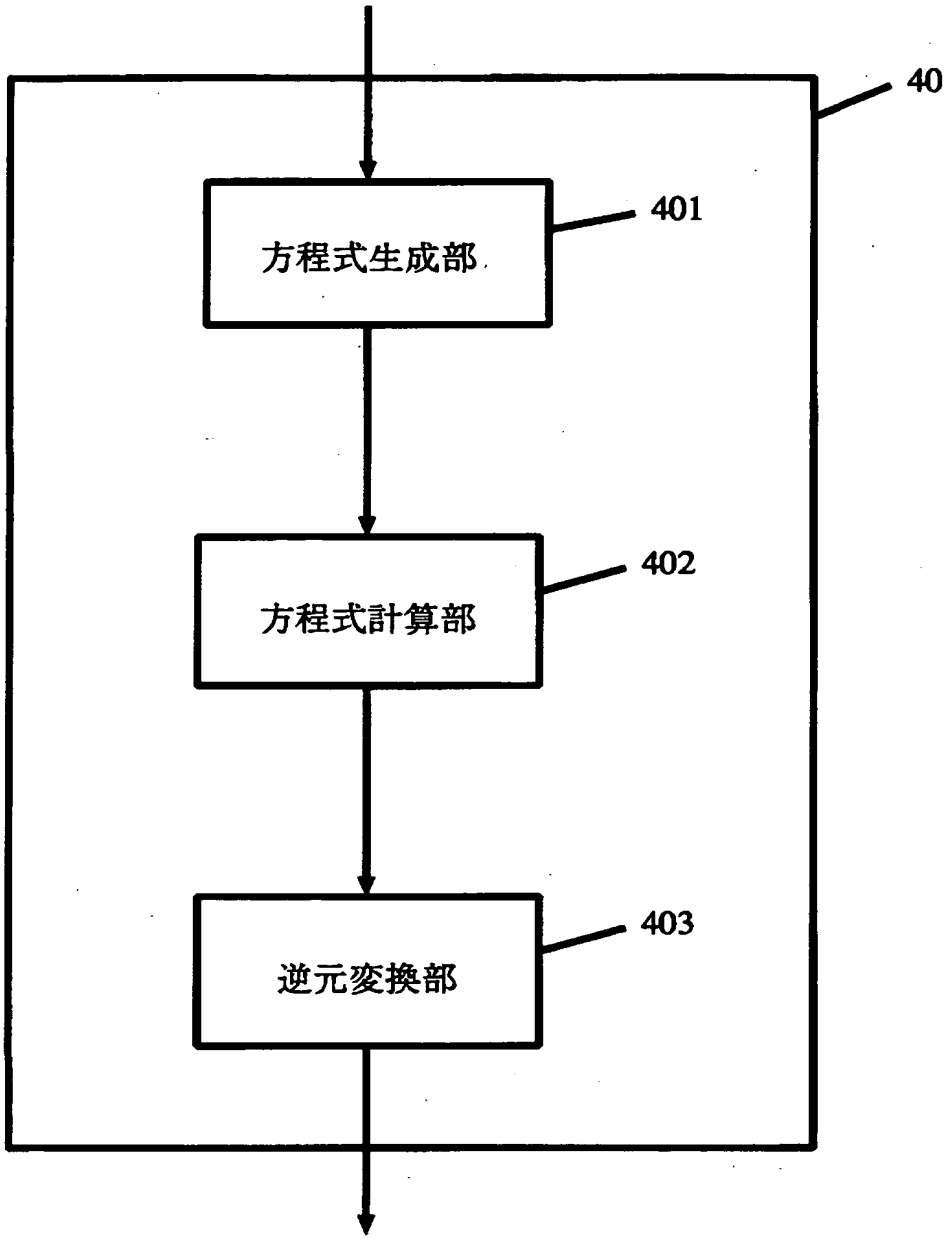
【図５】



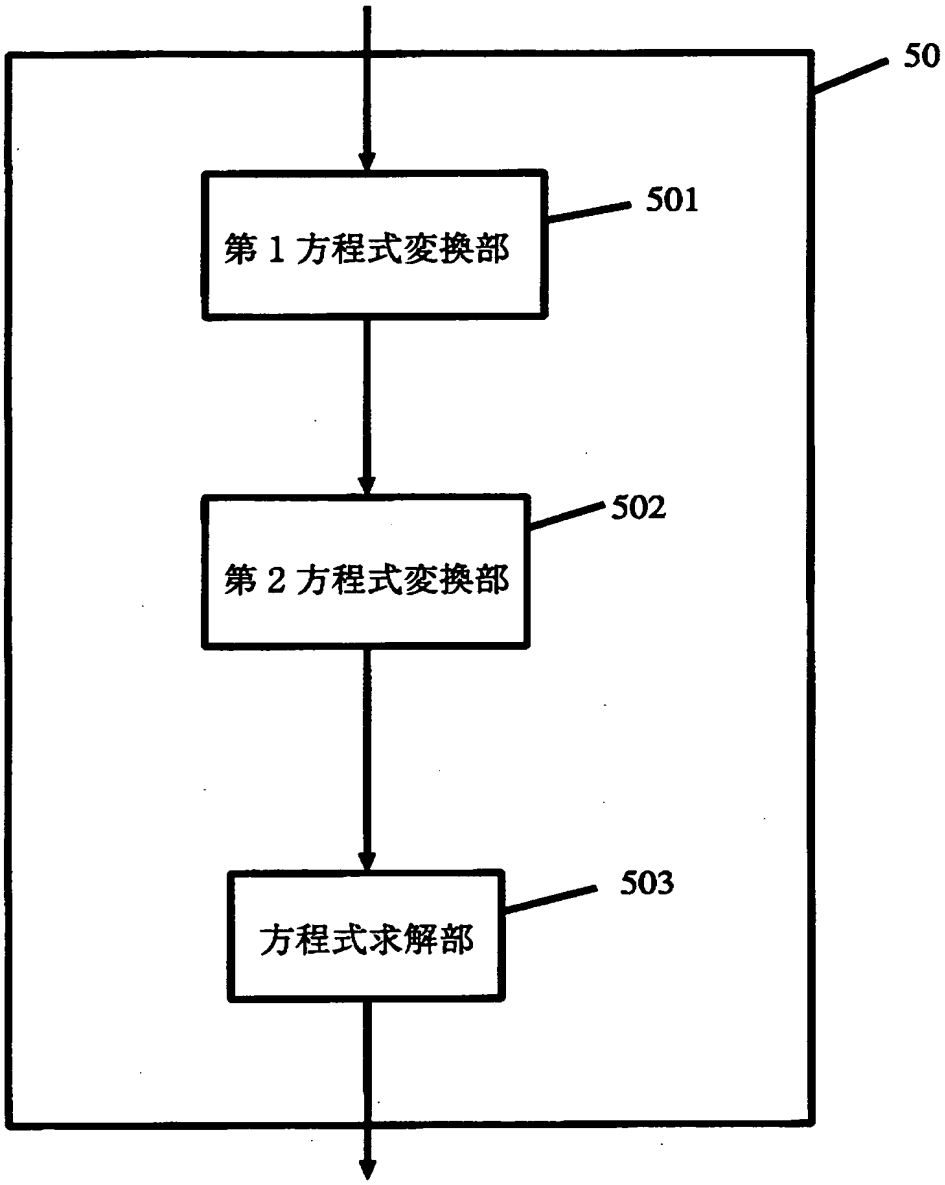
【図６】


301
302
303
ユーザA
管理センタ
ユーザB
x_A
S1
S2
$Y_A=x_A*G$
p, E, G
p, E, G, Y_A
S3
S4
乱数kを生成
S5
S6
$R_1=(r_x, r_y)=k*G$
S7
$s\times k=m+r_x\times x_A \bmod r$
からsを計算
S8
m, R_1, s
S9
$s*R_1=m*G+r_x*Y$
が成立するか判定

【図７】



【図８】



【書類名】　要約書

【要約】

【課題】　高速に有限体上の連立方程式の解を求める有限体上の演算装置を提供することにより、拡大体の逆元演算の計算時間を短縮し、高速な暗号システムを構築することを目的とする。

【解決手段】　本発明は、有限体GF(p)(p:素数)の連立方程式の解を求める有限体上の演算装置であって、連立方程式を行列とベクトルで表現する第１方程式変換部と、前記行列を三角化変換する第２方程式変換部と、三角行列の対角成分のGF(p)上の逆元を求める逆元演算部と、三角行列及びベクトルと、前記逆元を用いて前記連立方程式の解を求める方程式求解部を備え、前記第２方程式変換部では、前記有限体の逆元演算を行わないことを特徴とする。

【選択図】　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００５８２１〕

１．変更年月日　　１９９０年　８月２８日
［変更理由］　新規登録
住　所　　大阪府門真市大字門真１００６番地
氏　名　　松下電器産業株式会社